EXTENSIBLE FIRMWARE INTERFACE VIRUS SCAN

ABSTRACT

A secure method for implementing virus protection on a computer system having an Extensible Firmware Interface (EFI) and a basic input and output system (BIOS). The computer system has a hard disk, and a nonvolatile random access memory (NVRAM), such as a read-only-memory or flash device. To implement the functionality provided by the present invention, a command is added to the command shell of the Extensible Firmware Interface and stored in the NVRAM. This command automatically copies the boot sector of the hard disk to the NVRAM when the computer system is initialized. The boot sector of the hard disk is automatically read back from the NVRAM on each boot, which bypasses the boot sector access of the hard disk during system initialization, thus protecting and eliminating potential viruses. An field may be added to a BIOS SETUP routine that allows a user to enable or disable reading the boot record from NVRAM on boot. In implementing this, the BIOS SETUP routing is run, and the user is prompted to enable or disable reading the boot record from NVRAM on boot. The command shell of the EFI may also be modified to include a command to include a security signature input field. At the appropriate time during execution of the Extensible Firmware Interface the security signature input field is displayed to a user. The required signature is then input by the user prior to updating the stored boot sector.